# Incident handler's journal

## Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

| **Date:**<br>Tuesday 9am | **Entry:**<br>1 |
|---|---|
| Description | A small U.S. healthcare clinic experienced a ransomware attack. An employee opened a phishing email containing a malicious attachment. Once the attachment was downloaded, it installed malware that encrypted critical organizational data. A ransom note was displayed, demanding payment in exchange for a decryption key. |
| Tool(s) used | Not specified in the scenario, but common tools for response may include: antivirus software, network monitoring tools, endpoint detection and response (EDR), and backup recovery tools. |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who** caused the incident? An organized group of unethical hackers.<br>● **What** happened? The employee downloaded a malicious attachment from a phishing email, which led to ransomware being deployed.<br>● **When** did the incident occur? Tuesday at approximately 9:00 a.m. |

| | |
|---|---|
| | ● **Where** did the incident happen? At a small U.S. healthcare clinic specializing in delivering primary care services.<br>● **Why** did the incident happen? An employee opened a phishing email without recognizing it as suspicious, allowing malware to install and encrypt files. |
| Additional notes | Include any additional thoughts, questions, or findings.<br>Why weren't employees trained to detect and avoid phishing attempts?<br>Was antivirus or email filtering in place to block malicious attachments?<br>This incident highlights the need for user awareness training, endpoint protection, and a solid incident response plan. |

| | |
|---|---|
| **Date:**<br>July 12, 2025 | **Entry:**<br>2 |
| Description | Investigated a Suricata alert triggered by suspicious inbound traffic over HTTP. |
| Tool(s) used | Suricata, Wireshark |

| | |
|---|---|
| The 5 W's | - **Who:** The suspicious IP `198.51.100.24` triggered the alert.<br>- **What:** Suricata detected an HTTP GET request matching SID `12345`.<br>- **When:** Alert occurred at 03:42 UTC on July 12.<br>- **Where:** Target was internal web server `10.0.0.15` on port 80.<br>- **Why:** The request matched a known exploit pattern (rev:2) in the Suricata signature. |
| Additional notes | Reviewed packet capture with Wireshark to confirm suspicious content. Marked as low-priority after no exploit payload was found. |

| | |
|---|---|
| **Date:**<br>July 14, 2025 | **Entry:**<br>3 |
| Description | Used Splunk to perform a raw log search and identify failed SSH login attempts. |
| Tool(s) used | Splunk |
| The 5 W's | None |

| | |
|---|---|
| Additional notes | Query: `index=linux_logs "failed password"`<br>Revealed a brute-force login pattern from one IP. Recommend firewall rule update. |

| | |
|---|---|
| **Date:**<br>July 15, 2025 | **Entry:**<br>4 |
| Description | Investigated an alert related to SYN flooding detected on web server logs. |
| Tool(s) used | TCPDump, Wireshark |
| The 5 W's | **Who:** Multiple external IPs continuously sent SYN packets to `198.18.0.11`.<br>**What:** SYN flooding indicated a potential DDoS attempt.<br>**When:** Spikes were observed between 1–2 PM on July 15.<br>**Where:** The targeted system was a public-facing HTTP server.<br>**Why:** Attack intended to exhaust server resources via TCP half-open connections. |
| Additional notes | Captured packets and used Wireshark's flow graph to visualize connections. |

| | |
|---|---|
| | Confirmed as simulated attack in lab. |